

## **REMARKS**

Claims 1-3, 6-69, and 71-73 are pending in the application.

### **35 U.S.C. § 103 Rejections:**

Claims 1-3, 6-13, 16-20, 26-27, 30-31, 46-61 69, and 71-73 were rejected as being unpatentable over Beach, U.S. Patent Application Publication 2001/0055283, in view of Edwards, U.S. Patent Application Publication 2004/0059825. Claims 14-15, 21-25, 28-29, 32-35, 39-45, 62, and 65-68 were rejected under 35 U.S.C. § 103(a) as being unpatentable over Beach in view of Edwards and in further view of Park, U.S. Patent Application Publication 2004/0146158. Claims 36-38 and 63-65 were rejected under 35 U.S.C. § 103(a) as being unpatentable over Beach in view of Edwards and in further view of Campbell, Non-Patent Literature, November 2000. Applicant respectfully traverses these rejections.

**The prior art references, taken singly or in combination, fail to teach or suggest all of the elements of the independent claims.** Independent claim 1 recites, in pertinent part:

A method of performing encrypted WLAN (Wireless Local Area Network) communication, comprising the steps of ... operating a WLAN chip to perform data frame encapsulation and/or decapsulation during said encrypted WLAN communication ... wherein said data frame encapsulation and/or decapsulation is performed by operating single-purpose hardware of said WLAN chip without executing software-implemented instructions of said driver software, wherein performing said encrypted WLAN communication further comprises obtaining a plurality of data frames intended for said data frame encapsulation from driver software.

Independent claims 46, 69, and 71 recite similar combinations of features.

The Examiner contends that “wherein said data frame encapsulation and/or decapsulation is performed by operating single-purpose hardware of said WLAN chip without executing software-implemented instructions of said driver software” is taught by Beach in paragraphs [0060]-[0062] and [0110]. Applicant respectfully disagrees.

In the ‘Response to Arguments’ section of the present office action, the Examiner makes the following contention:

Beach teaches or suggests data frame encapsulation based on conforming with the IEEE standard. IEEE 802.11 discloses data frame encapsulation/decapsulation as it describes how MAC frames should be constructed in Chapter 7 of IEEE 802.11 standard (1999).

Accordingly, the Examiner is relying on a reference in Beach to the IEEE 802.11 standard, and that, by virtue of this reference, contends that the combined references teach or suggest all of the limitations of the claims, including the limitation of “operating a WLAN chip to perform data frame encapsulation and/or decapsulation during said encrypted WLAN communication” as recited in claim 1. Applicant respectfully disagrees with the Examiner’s contention.

Data frame encapsulation/decapsulation was first addressed in IEEE 802.11i. This is noted in paragraph [0007] of U.S. Patent Application Publication 20050172119 (which is the corresponding publication of the present application):

[0007] In order to address existing security gaps of the 802.11 standard's native security, i.e. the WEP (Wired Equivalent Privacy) protocol, the 802.11i security standard was developed. This

enhanced security standard relies on the 802.1x standard for port-based access control, and the TKIP (Temporal Key Integrity Protocol) and CCMP (Counter-mode Cipher block chaining Message authentication code Protocol) protocols for data frame encapsulation and decapsulation. 802.1x provides a framework for WLAN station authentication and cryptographic key distribution, both features originally **missing** from the 802.11 standard. The TKIP and CCMP protocols are cipher protocols providing enhanced communication security over the original WEP protocol, the TKIP protocol being targeted at legacy equipment, and the CCMP protocol being targeted at future WLAN equipment. (Emphasis added).

The IEEE 802.11i standard was first ratified in 2004. However, Beach was filed in 2001. Similarly, each of the other references pre-dates the ratification of IEEE 802.11i. Accordingly, the reference to the IEEE 802.11 standard by Beach is a reference to an earlier standard that did not include data frame encapsulation/decapsulation. While chapter 7 of the IEEE 802.11 revision cited by the Examiner specifies frame formats, it does not disclose data frame encapsulation/decapsulation. Furthermore, none of the other cited references, taken singly or in combination with Beach, teach or suggest data frame encapsulation/decapsulation. Thus, a reference to the IEEE 802.11 standard by the various cited references is insufficient to show the limitations of data frame encapsulation/decapsulation, since each of the references predates the IEEE 802.11i standard in which these particular features were first implemented. **Accordingly, even if the references were combined as proposed by the Examiner, the combination of features would still fail to include the limitation of “operating a WLAN chip to perform data frame encapsulation and/or decapsulation during said encrypted WLAN communication” as recited in claim 1 and similarly recited in other ones of the independent claims.**

Notwithstanding the above, Beach fails to teach or suggest data frame encapsulation/decapsulation using “single-purpose hardware of said WLAN chip **without** executing software-implemented instructions of said driver software.” The Examiner contends that Beach teaches this limitation in paragraph [0059], which states the following:

[0059] The following optional (higher or lower) level MAC functions can be placed in either the higher or lower level categories.

Paragraphs [0060]-[0063]

[0060] Wired Equivalent Privacy encryption/decryption (WEP)

[0061] Fragmentation/Reassembly

[0062] Data Movement

[0063] Power Save Polling Support (PSP)

Nothing in paragraph [0059] or subsequent paragraphs [0060]-[0063] of Beach provides any discussion whatsoever of data frame encapsulation or decapsulation that is performed using single-purpose hardware of a WLAN chip without executing software-implemented instructions of driver software. Beach provides no additional teaching or suggestion of these limitations elsewhere. Furthermore, none of the other cited references provide any teaching or suggestion of these limitations that, taken alone or together with Beach, would result in the claimed combinations of features. **Accordingly, the various combinations of Beach and the other cited references fails to teach or suggest “operating a WLAN chip to perform data frame encapsulation and/or decapsulation during said encrypted WLAN communication ... wherein said data frame encapsulation and/or decapsulation is performed by operating single-purpose hardware of said WLAN chip without executing software-implemented instructions of**

**said driver software,” as recited in claim 1 and similarly recited in the other independent claims.**

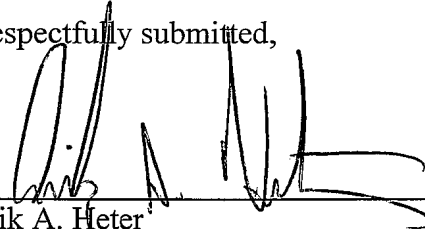
For at least the reasons given above, Applicant submits that Beach in view of Edwards (and in further view of the other cited references) fails to teach or suggest all of the limitations of the independent claims. Accordingly, removal of the 35 U.S.C. § 103(a) rejections is respectfully requested.

### **CONCLUSION**

Applicant submits the application is in condition for allowance, and an early notice to that effect is requested.

If any fees are due, the Commissioner is authorized to charge said fees to Meyertons, Hood, Kivlin, Kowert, & Goetzel, P.C. Deposit Account No. 501505/5800-00601/EAH.

Respectfully submitted,



Erik A. Heter  
Reg. No. 50,652  
AGENT FOR APPLICANT(S)

Meyertons, Hood, Kivlin, Kowert, & Goetzel, P.C.  
P.O. Box 398  
Austin, TX 78767-0398  
Phone: (512) 853-8800

Date:

8/6/08